DOMAINTOOLS®

2019 CYBERSECURITY REPORT CARD

ORGANIZATIONS RATE THEIR SECURITY POSTURE AND DEMONSTRATE TRENDING BEST PRACTICES

2019 has been a year filled with major data breaches making headline news and exposing billions of records of personal data. From the outside looking in, it's easy to draw the conclusion that cybersecurity is in a state of constant failure.

Those on the cyber defense frontlines that work day-in and day-out to implement security solutions and practices are, however, reporting real progress being made in their organizations toward a more mature security posture that is resulting in a year-over-year decline in incidences of breaches.

This paper outlines the results of the DomainTools third annual Cybersecurity Report Card Survey. More than 500 security professionals from companies ranging in size, industry, and geography were surveyed about their security posture and asked to grade the overall health of their programs. Their responses built on the results of the previous 2018 and 2017 Report Cards and further strengthened and supported numerous trends that have been playing out year-over-year.

SUMMARY HIGHLIGHTS

The report finds that confidence in cybersecurity programs continues to grow. Thirty percent of respondents gave their program an "A" rating, doubling over two years from 15 percent in 2017. The incidence of reported security breaches also continues to decline year-over-year. The percentage of organizations that have been breached in the past 12 months has dropped from 26 percent in 2017 to 15 percent in 2019, according to the findings. Automation is playing an increasingly important role in securing organizations, with 88 percent strongly agreeing or agreeing that automation has improved their staff's technical skills and general knowledge of cybersecurity. While 22 percent of organizations employ a high level of automation, that number doubles to 45 percent of organizations that give themselves an "A" grade.

KEY FINDINGS

A TIPPING POINT YEAR

Cybersecurity report card grades showed a sharp increase in improvement in 2019, with 30 percent giving their programs an "A," up nearly 10 percent from 2018. Almost half of all respondents stand solidly as a "B," with an overall decline in grades "C" through "F," showing improvement across the board. Along with this comes a five percent decrease in organizations that report having been breached in the past 12 months.

SOCS LEAD TO BETTER OUTCOMES

A sign of security programs evolution, the use of in-house SOCs are on the rise and elevating security across the organization. More than half (53%) of organizations now carry out security operations with a full in-house SOC, up 10 percent over 2017. Grade "A" respondents overwhelmingly rely on in-house SOC to keep their grades high, with 78 percent reporting their implementation.

AUTOMATION KICKS IN

Automation up levels the capabilities of security analysts, removing rote work and enabling security professionals to focus on high-priority vulnerabilities and overall network security. Automation is vastly viewed as positive among respondents, with 88 percent strongly agreeing or agreeing that automation has improved their staff's technical skills and general knowledge of cybersecurity.

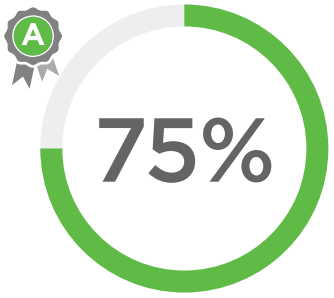
SHIFTING THE BALANCE OF POWER

Threat hunting and investigation takes security proactive. Organizations are on average spending more time hunting threats in their network. In 2017 and 2018, roughly a third of organizations were spending less than five hours per week on threat hunting. That number has dropped to a fifth (20.7%) as organizations move towards increasing the amount of time for threat hunting.

A TIPPING POINT YEAR

Over the past three years, organizations have steadily improved their cybersecurity grades. Beginning in 2017, only 15 percent of respondents gave their security programs an "A," with that number doubling to 30 percent this year. In 2017 and 2018, respondents listed the need for more budget as the number one hurdle to achieving an "A" grade. This year the need for more staff was the number one request. The increase in use of automation and other security tools over the years corresponds with budget requests being met. Now that teams have the tools, they are feeling the IT skills talent shortage.

With year-over-year increases in the use of automation, in-house SOC and threat intelligence platforms, analysts are able to detect and respond to threats faster. Slightly over half (51%) of organizations with an "A" grade are able to detect active or suspected cyber attacks several times throughout the day. This increase in awareness and responsiveness parallels a decline in reported breaches year-over-year, having dropped from 26 percent in 2017 to 15 percent this year.



Percentage of organizations detect an attack in less than a day

A TIPPING POINT YEAR (CONT)

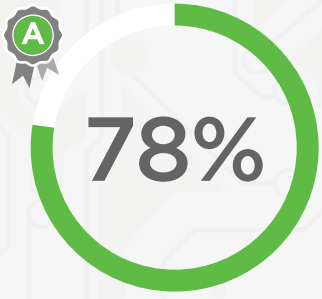
HOW WOULD YOU GRADE YOUR CYBERSECURITY SYSTEM?

HAS YOUR ORGANIZATION BEEN BREACHED IN THE PAST 12 MONTHS?

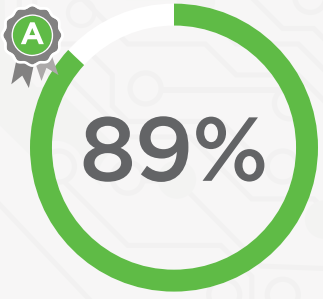
SOCS LEAD TO BETTER OUTCOMES

In-house SOCs are proving to be a key component of an organization's security posture and an indicator of the maturity of a security organization. Organizations with an in-house SOC seem to demonstrate advanced inspection capabilities, such as developing larger maps of threat infrastructure from a single indicator. While only 30 percent of organizations had this capability in 2017 and 2018, that number jumps to over half (51%) this year. Grade "**A**" respondents especially value this capability, with 70 percent regularly performing these deeper analyses.

With an increase of in-house SOCs comes a rise in formalized training for security staff. Companywide programs to keep IT staff up to date on the latest threats and trends are up over 10 percent since 2017 to 63 percent today. The value that formalized training brings to an organization's security program is becoming more recognized. In 2017, twenty percent of respondents claimed no use or need for a company-wide training program to continually educate IT staff—that number has decreased to only 10 percent today.

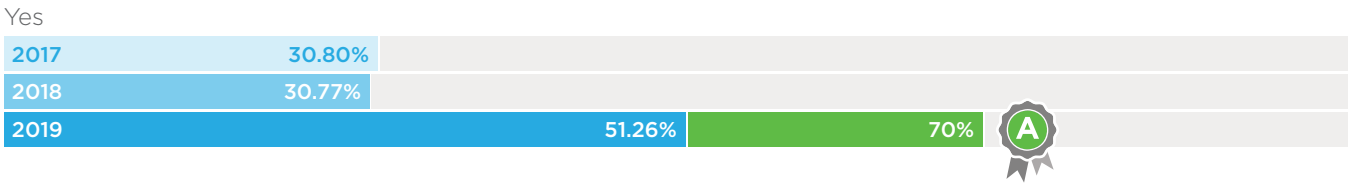


Percentage have a full in-house SOC

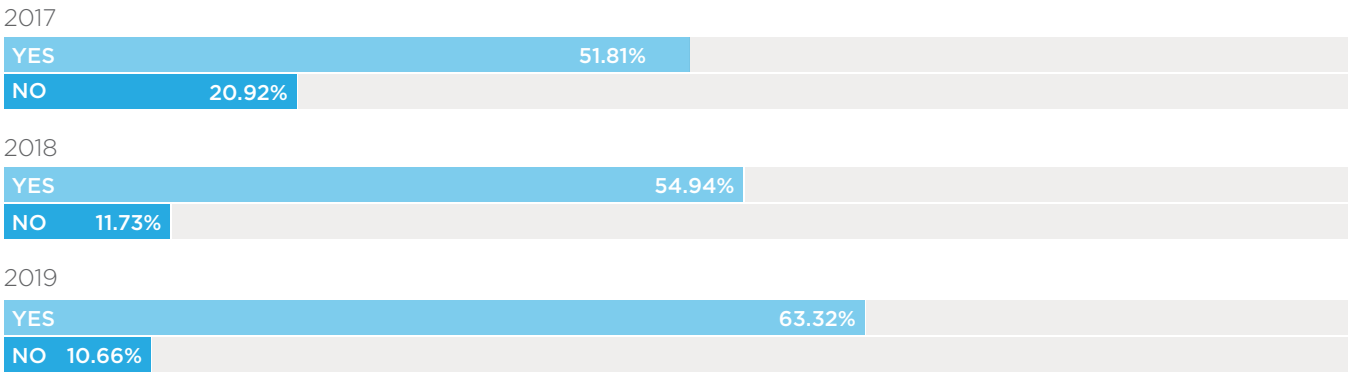


Percentage have formalized training programs for security staff

WE USE A VARIETY OF SYSTEMS TO MANUALLY DEVELOP A LARGER THREAT MAP.



DO YOU HAVE A FORMALIZED COMPANYWIDE TRAINING PROGRAM TO KEEP YOUR SECURITY STAFF UP-TO-DATE ON THE LATEST THREATS AND TRENDS?

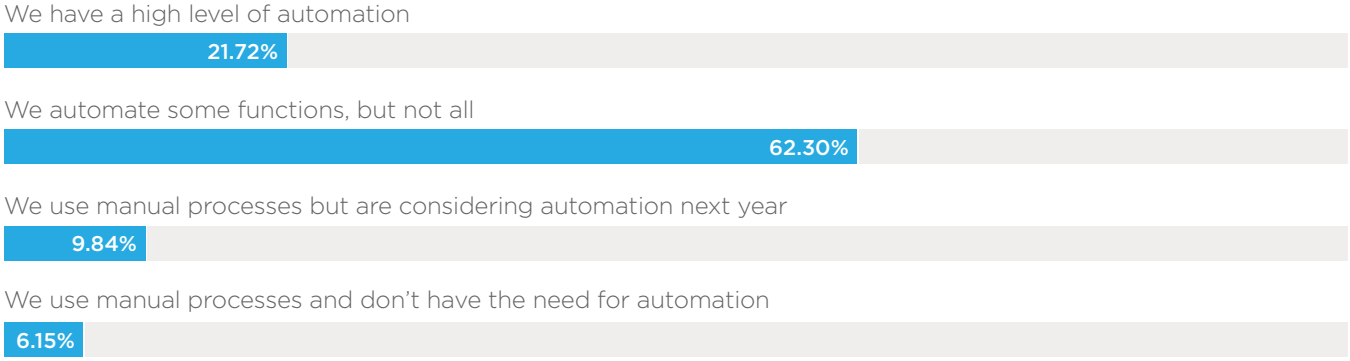


AUTOMATION KICKS IN

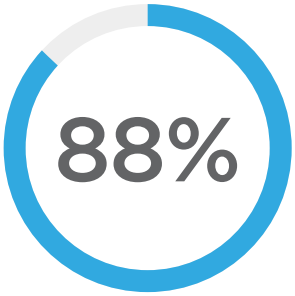
In the world of cybersecurity, every second matters. Being able to quickly detect and investigate threats is fundamental to an organization's ability to prevent them. Over half (51%) of grade "**A**" organizations have the ability to detect active or suspected cyber attacks multiple times per day.

Automation is a critical component of any well-performing security program. With organizations being relentlessly attacked from every possible angle, even the most highly skilled security teams cannot handle today's security processes manually. Automation supports analysts by removing mundane, time-intensive tasks so security professionals can focus on higher-level threat analysis and proactive prevention measures.

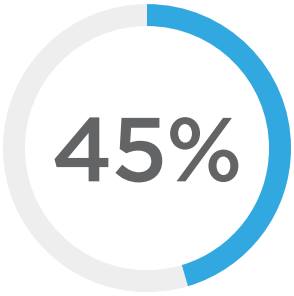
WHAT IS YOUR LEVEL OF SECURITY AUTOMATION?



AUTOMATION KICKS IN (CONT)



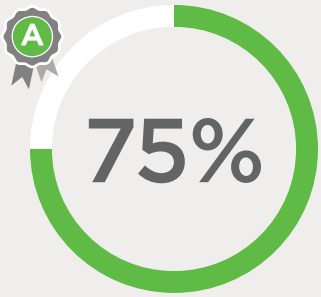
Percentage agree automation has improved their staff's technical skills and general knowledge of cybersecurity



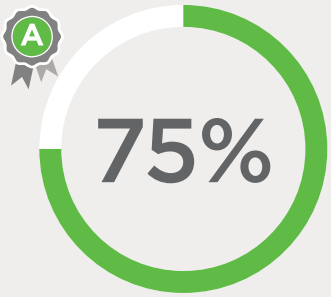
Percentage have a high level of automation

Percentage automate some but not all functions

Percentage use Orchestration



Percentage use Anti-Phishing or other messaging security software



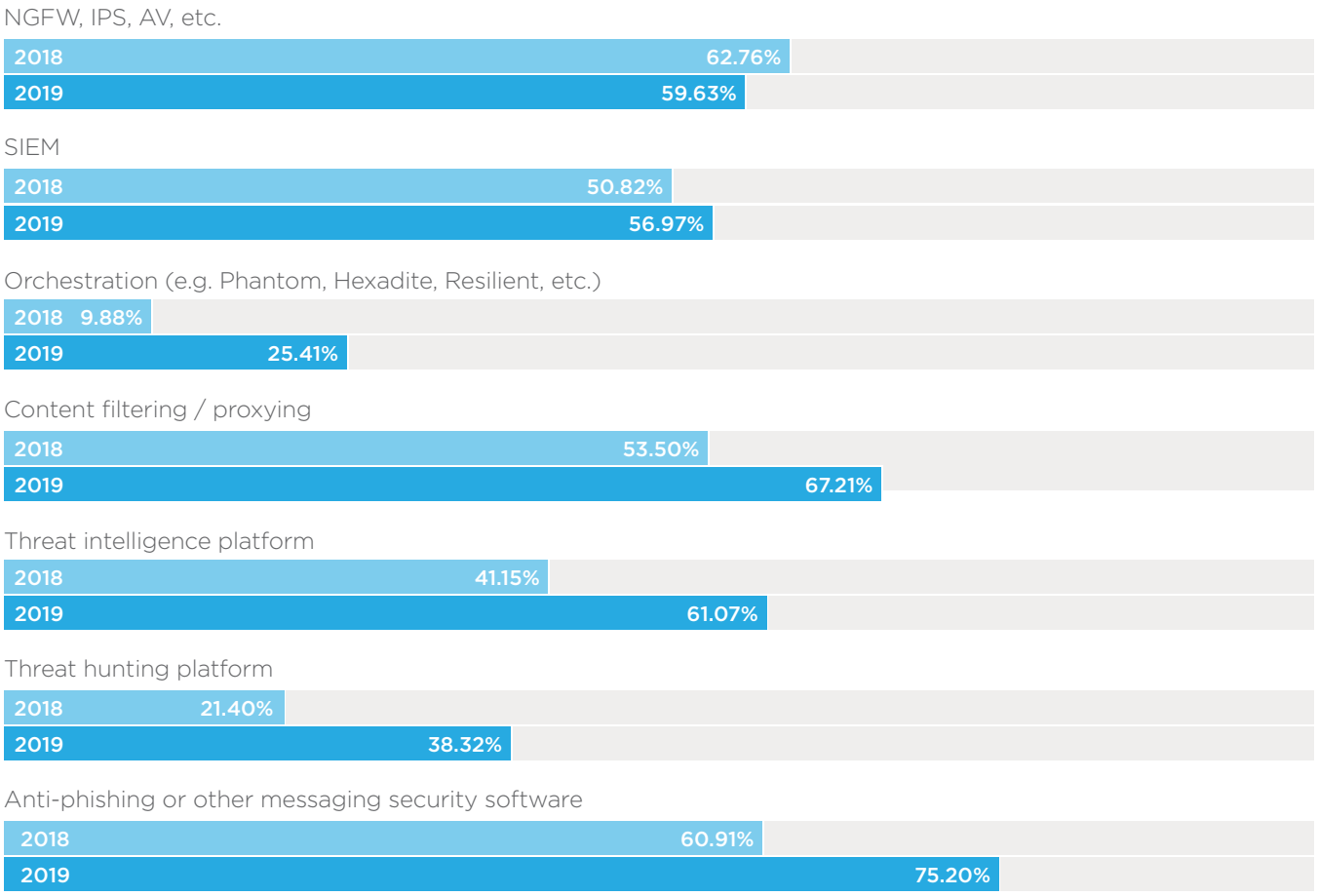
Percentage use a Threat Intelligence Platform

SHIFTING THE BALANCE OF POWER

Organizations are showing a greater emphasis on proactive threat hunting. As mentioned earlier, now only one-fifth of survey respondents (as opposed to previous years of one-third) spend less than five hours per week hunting threats; another third spends anywhere from six to 25 hours, and nearly 20 percent spend more than 60 hours per week. Six percent of respondents said they do not threat hunt at all. Additionally, a total of 11 percent of survey respondents identify their title as "Threat Hunter," up five percent since 2018, demonstrating that organizations are dedicating resources to build out this emerging role that they see as a growing necessity.

There have also been steady increases in the sophistication of organizations' threat hunting capabilities. In 2017, 38 percent of organizations did not have the capability to expand from one indicator to a larger map of threat infrastructure—today that number is down to 30 percent. Nearly 20 percent (18.41%) of organizations have one product to view their larger threat infrastructure, and 51 percent utilize a variety of systems to manually develop a larger threat map.

WHICH TOOLS DO YOU USE AS PART OF YOUR ORGANIZATION'S DEFENSE APPROACH?



COMMON ATTACKS SEE SHIFT TO BEC

Common threat vectors remain steady year over year with Malware and Spearphishing at the top of the list; Business Email Compromise makes it to the top 3 this year.

41%
Percent of organizations detect active or suspected cyber attacks several times a day (vs. week, month or year and a rise over 2018)

12.8%
On the steady decline: DDoS attacks

THE TOP THREE MOST COMMON ATTACKS DETECTED ARE:

- 74% - MALWARE
- 61% - SPEARPHISHING
- 40% - BUSINESS EMAIL COMPROMISE

KEYS TO SUCCESS IN 2020

How can organizations improve their grades next year? According to the data, organizations seem to be moving steadily in the right direction. Three specific areas of interest that may have the most impact would be hiring more security staff, creating an in-house SOC, and investing time and resources to run deep analysis on malware for threat intelligence.

As noted previously, of the respondents who did not make the "**A**" grade this year, the need for more staff was the number one request to increase their standing. Previous years have all indicated the need for more budget as the number one culprit. Budget requests actually fell to third place this year, as more respondents requested increased automation after more trained staff.

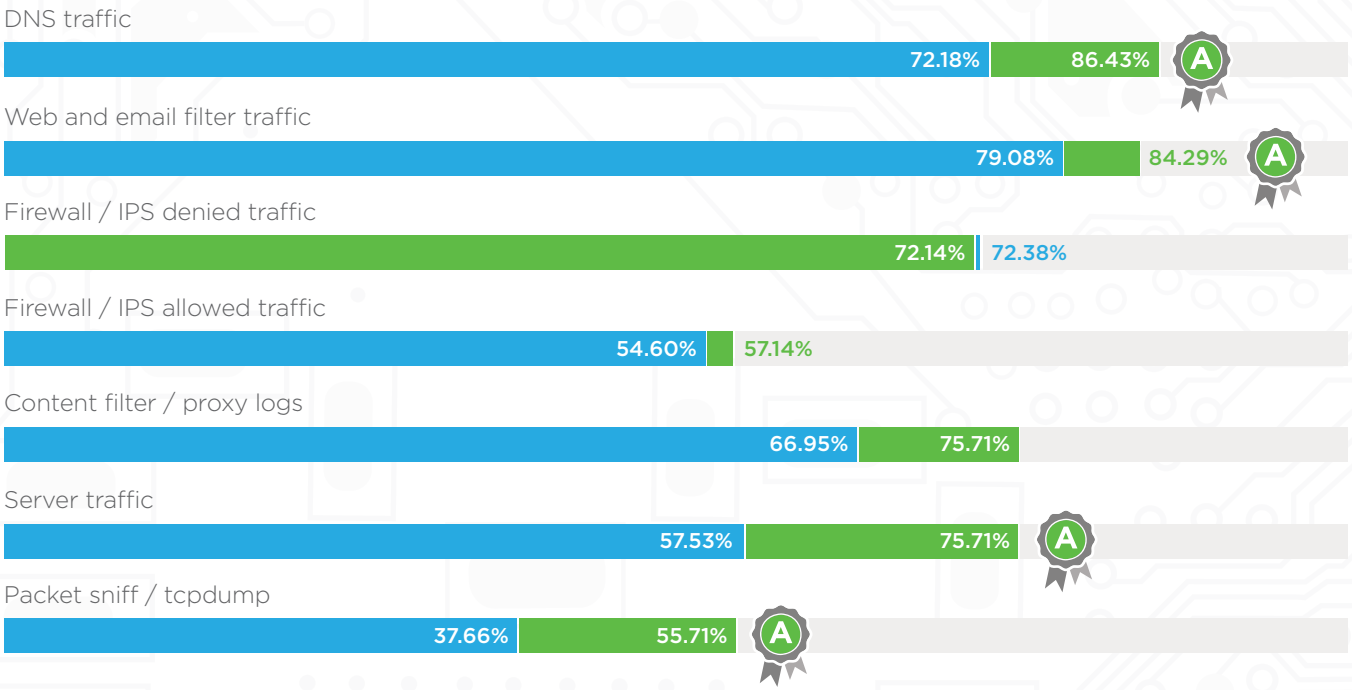
The request for greater cooperation and security education among employees has been on a year-over-year decline, suggesting an increasing prioritization to support security efforts throughout the organization.

As malware remains the most common and persistent attack vector, 60 percent of organizations now have in-house malware expertise. Analyzing these attacks more closely pays off with valuable threat intelligence that organizations need to make them more secure in the future. Sixty-seven percent of Grade "**A**" companies spend time on malware analysis, up 10% from other respondents. Ninety percent of Grade **"A"** companies follow up on forensic clues from phishing emails, such as domain name, IP address, or email address, a 15 percent increase over the average. As a second priority, 82 percent of Grade "**A**" organizations analyze evidence of data exfiltration or unexplained outbound connections to questionable destinations.

"Unfortunately, security teams report they are more short-staffed than ever, with the need for more staff as the number one hurdle to achieving an "A" grade in 2019, overtaking budget issues from previous years."

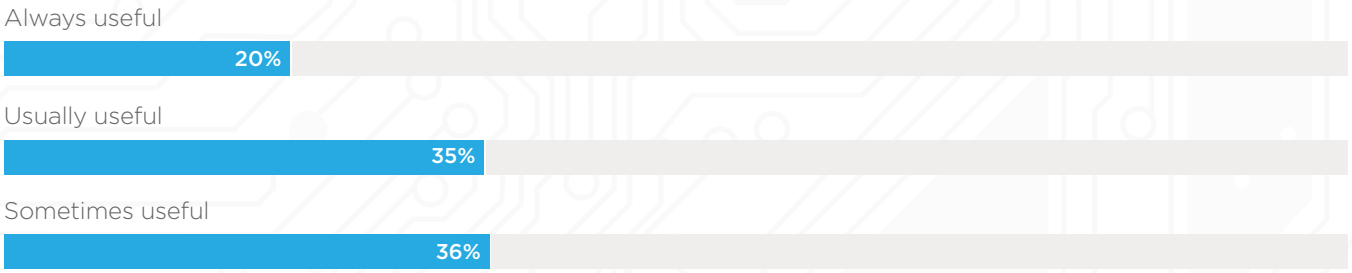
— Tarik Saleh, Senior Security Engineer and Malware Researcher

WHAT TYPE OF DATA DO YOU LOG FOR LATER FORENSIC REVIEW?

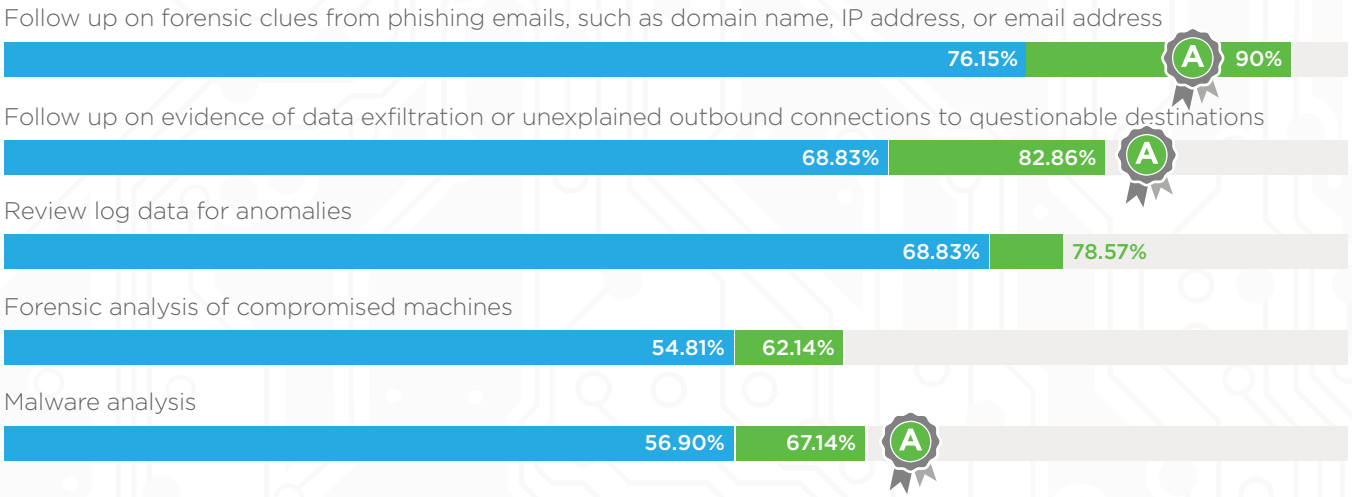


KEYS TO SUCCESS IN 2020 (CONT)

DRILLING DOWN ON THE IP ADDRESS OR DOMAIN NAME IN INVESTIGATING OR STOPPING A CUSTOMIZED ATTACK LEADS TO INCREASED ORGANIZATIONAL SECURITY.



WHEN INVESTIGATING ATTACKS, DO YOU DO THE FOLLOWING?

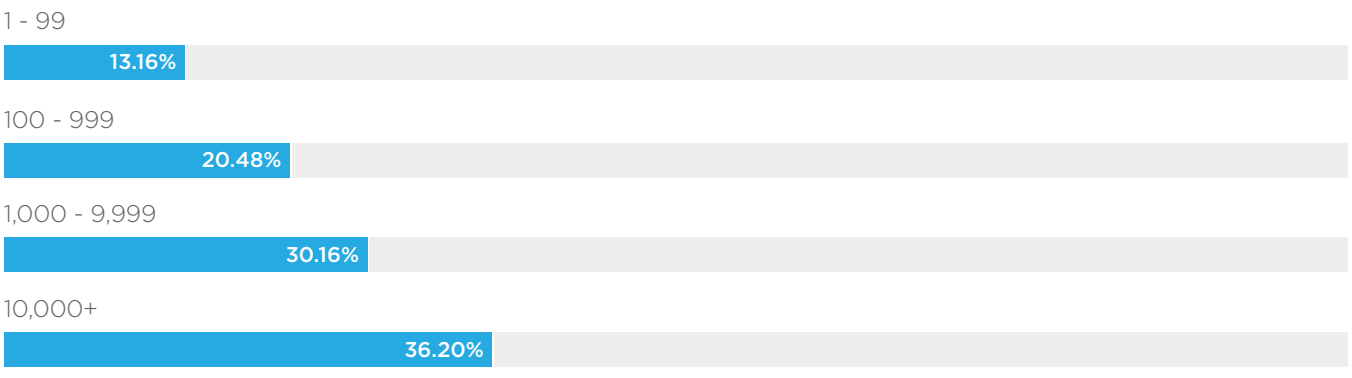


METHODOLOGY

The survey was conducted by DomainTools in September 2019, and polled 525 global security professionals and executives working in finance, government, healthcare, retail, technology and other industries in organizations of up to 10,000+ employees.

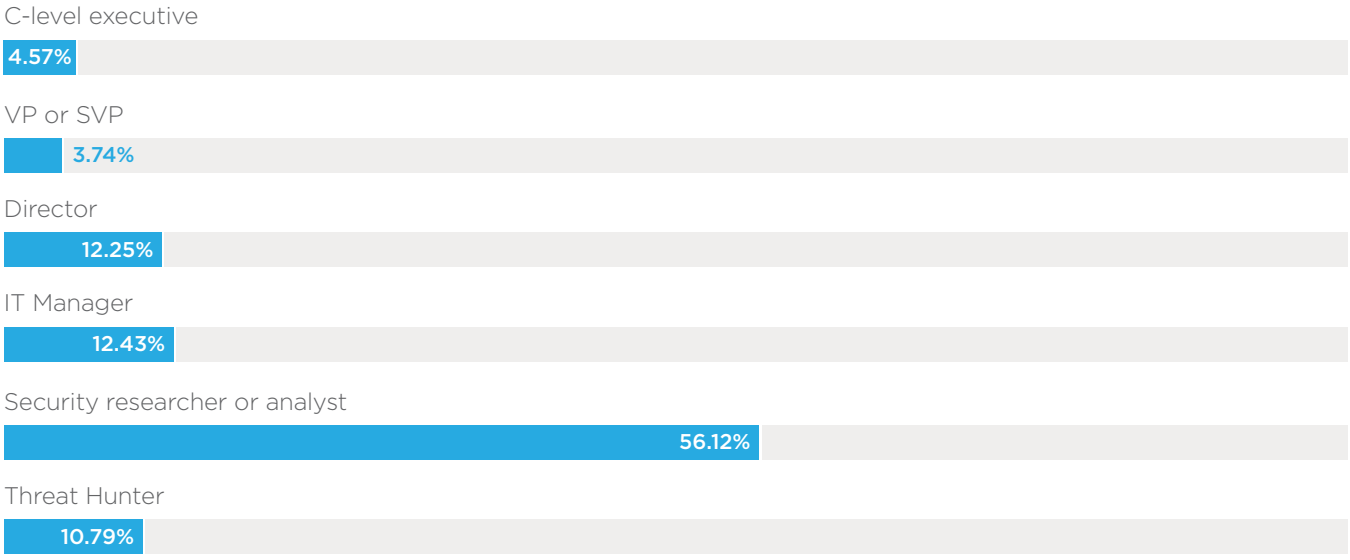
Regions include North America, EMEA, APAC and LATAM. A breakdown of the respondents' titles, roles and industries are provided below.

HOW LARGE IS YOUR ORGANIZATION?

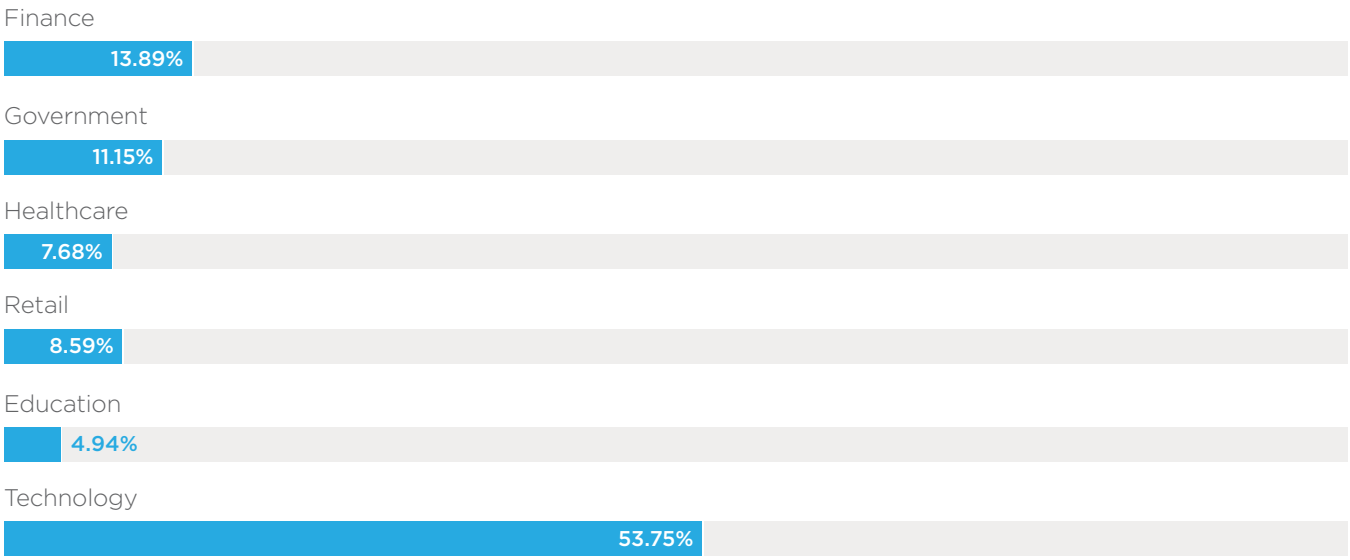


METHODOLOGY (CONT)

WHAT IS YOUR JOB TITLE?



WHAT IS YOUR INDUSTRY?



ABOUT DOMAINTOOLS

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work. Learn more about how to connect the dots on malicious activity at http://www.domaintools.com or follow us on Twitter: @domaintools.